МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Информационная безопасность организаций»
для студентов направления подготовки 38.04.01 Экономика
направленность (профиль) «Экономическая безопасность и управление рисками»

2026

Методические указания по дисциплине «Информационная безопасность организаций» содержат задания для студентов, необходимые для проведения практических занятий.

Проработка практических заданий позволит сформировать у студентов системные представления информационной безопасности организаций. Предназначены для студентов направления подготовки 38.04.01 Экономика направленность (профиль) «Экономическая безопасность и управление рисками».

Содержание

1. Цели и задачи изучения дисциплины

Целью освоения дисциплины является формирование профессиональных (ПК-5) компетенций у магистров по направлению подготовки 38.04.01 «Экономика» направленность (профиль) Экономическая безопасность и управление рисками. Основная цель курса «Информационная безопасность организаций» заключается в состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

Задачами освоения дисциплины являются: сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния; изучение порядка организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации; получение практических навыков анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-5. Способен разрабатывать и обосновывать финансово-экономические показатели деятельности предприятия и методики их расчета с целью формирования эффективной стратегии развития и функционирования хозяйствующего субъекта используя цифровые технологии	ИД-3 ПК-5. Анализирует показатели финансово-хозяйственной деятельности организации с использованием цифровых технологи	Применяя знания об информационной безопасности, информационных угрозах, и возможных последствиях, использует их для принятия обоснованных решений по выбору политики информационной безопасности и оценки эффективности инвестиций в информационную безопасность

3. Задания к практическим работам

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 1

Понятие информационной безопасности. Основные составляющие

Теоретическая часть

Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Каждый прорыв человечества в будущее не освобождает его от груза прошлых ошибок и нерешенных проблем. Когда экономические войны из-за интеграции национальных экономик стали слишком опасными и убыточными, а глобальный военный конфликт вообще способен привести к исчезновению жизни на планете, война переходит в иную плоскость - информационную.

Информационная война - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Информационное воздействие - акт применения информационного оружия.

Информационное оружие - комплекс технических и других средств,

методов и технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;

- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;

- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;

- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий.

Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации. Под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее

могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угроз случайные, или непреднамеренные. Их источником могут быть выход из строя аппаратных средств, неправильные действия работников информационные системы (ИС) или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д. Такие угрозы тоже следует держать во внимании, т.к. ущерб от них может быть значительным. Однако в данной работе наибольшее внимание уделяется угрозам умышленным, которые в отличие от случайных преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют "компьютерным пиратом" (хакером).

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С помощью различного вида уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации понимается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Информационная безопасность включает:

- состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;

- состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;

- состояние информации, при котором исключается или существенно

затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;

- экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);

- финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

Вопросы к практическому занятию:

1. Назовите особенности современного информационного общества.
2. Какие элементы информационной инфраструктуры Вы знаете?
3. Что понимается под угрозой безопасности информации?
4. Дайте определение информационной безопасности на предприятии.
5. Назовите объекты информационной безопасности на предприятии.
6. Какие обеспечивающие подсистемы включает система защиты информации?

7. Назовите особенности экономической информации.

8. В чем отличия понятий информационный ресурс, продукт и услуга?

9. Как определяется цена информационного продукта?

10. Что такое конфиденциальность, целостность и доступность информации?

11. Какая информация компании не может быть отнесена к коммерческой тайне?

12. Информационная безопасность. Доступность, целостность, конфиденциальность.

13. Защита информации, субъект информационных отношений, неприемлемый ущерб.

14. Компьютерное преступление, жизненный цикл информационных систем.

15. Что такое персональные данные?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 2

Наиболее распространенные угрозы информационной безопасности и её составляющие

Теоретическая часть

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз

конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

Информационные угрозы могут быть обусловлены:

- естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины);
- человеческими факторами. Последние, в свою очередь, подразделяются на:
- угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные пр01раммы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за

недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

— угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение

сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование ресурсов; несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания.

Вопросы к практическому занятию:

1. Назовите информационные угрозы для государства.
2. Какие создаются информационные угрозы для компании?
3. Что угрожает личности (физическому лицу)?
4. Назовите причины информационных угроз.
5. Какие действия и события нарушают ИБ?
6. Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ?

7. Назовите основные компьютерные вирусы.
8. Какие вы знаете компьютерные преступления?
9. Основные определения и критерии классификации угроз.
10. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
11. Основные угрозы доступности.
12. Основные угрозы целостности.
13. Основные угрозы конфиденциальности.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 3

Законодательный уровень информационной безопасности

Теоретическая часть

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Менеджмент информационной безопасности предполагает выделение нескольких ИБ:

1. Уровень международных профессиональных объединений, связанных со сферой информационных технологий, телекоммуникаций и информационной безопасности.
2. Уровень крупных компаний, работающих в сфере информационных технологий и в значительной мере определяющих состояние информационной безопасности в сообществе пользователей информационных систем, а также влияющих на безопасность различных элементов информационной инфраструктуры.
3. Государственный уровень - уровень государственных и межправительственных организаций, влияющих на жизнь общества, состояние правовой системы, развитие экономики и технологий.

4. Уровень отдельных компаний - сообщество пользователей информационных систем, заинтересованных в собственной информационной безопасности и обеспечивающих защиту имеющихся у них информационных ресурсов собственными силами.

Некоторые исследователи выделяют дополнительный промежуточный уровень - консалтинговые и внедренческие компании, учебные центры, работающие в сфере информационной безопасности и действующие как связующее звено между различными организационными уровнями.

Для каждого уровня указанной иерархии характерны свои задачи и специфичные методы организационной работы.

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции государства начали борьбу с ней при помощи традиционных норм о краже, присвоении, мошенничестве, злоупотреблении доверием и др. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений (например, воровство из квартиры - это одно, а копирование секретной компьютерной информации - это другое).

Несоответствие криминологической реальности и уголовно-правовых норм потребовало развития последних. Развитие это происходит в двух направлениях:

• более широкое толкование традиционных норм;

• разработка специализированных норм о компьютерных преступлениях.

Преступления, совершаемые с помощью компьютера в финансово-кредитной системе, в особенности отмывание денег, нажитых преступным путем, приняли мировой масштаб. Законодатели, стараясь обезопасить свои страны от его проникновения, издали ряд законов, направленных на организацию контроля государственными органами и банками вкладов и денежных переводов граждан. Что же предусматривается в этой связи в США:

- каждое финансовое учреждение должно предоставлять службе казначейства (агентству внутренних дел) декларацию для совершения различных банковских операций на сумму более 10 тыс. долларов;
- игорные дома с общим годовым доходом свыше одного миллиона долларов вносятся в список финансовых организаций, которые обязаны регистрировать денежные операции на сумму свыше 10 тыс. долларов;
- министр финансов уполномочен выплачивать вознаграждение лицам, которые предоставляют ему сведения (из первых рук) о нарушении финансовой дисциплины при совершении операций на сумму свыше 50 тыс. долларов. Вознаграждение ограничивается либо 25% конфискованной суммы, либо 150 тыс. долл.

Попытки регулирования отношений в сфере компьютерной информации уже не один десяток лет предпринимаются не только в США, но и в других развитых странах.

Российская действительность не является исключением и каждодневно приносит новые примеры преступлений в сфере информатизации и компьютеризации. Последние потребовали от российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации,

Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти,

принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Вопросы к практическому занятию:

14. Что составляет базу функционирования специализированных организаций в сфере информационной безопасности?

15. Назовите характерные черты организационной работы специализированных организаций в сфере информационной безопасности.

16. Что представляют собой альянсы крупных технологических компаний?

17. Перечислите типичные приемы организационной работы альянсов крупных технологических компаний.

18. Чем занимается Альянс по смарт-картам?

19. Какие задачи решает Альянс по безопасности сети Интернет?

20. О чем Доктрина информационной безопасности РФ (5 декабря 2016 г.)?

21. Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

22. О чем Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (с изм. на 2014 г.)?

23. Охарактеризуйте содержание статей 159(1-6), 272, 273, 274 УК.

24. Российское законодательство в области информационной безопасности.

25. Стандарты и спецификации в области информационной безопасности.

Задание для самостоятельной работы:

1. Сделайте доклад о деятельности одной из специализированных

организаций в сфере информационной безопасности.

2. Сделайте доклад о деятельности одной из международных организаций в сфере информационной безопасности.

3. Заполните таблицу.

Наименование международной организации	Основные задачи

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 4

Административный уровень информационной безопасности

Теоретическая часть

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Службы, организующие защиту информации на уровне предприятий (банков и др.):

- отдел экономической безопасности;
- служба безопасности персонала (режимный отдел);
- службы информационной безопасности;

- отдел кадров.

Для создания и поддержания необходимого уровня информационной безопасности в фирме разрабатывается система соответствующих правовых норм, представленная в следующих документах:

- Уставе и/или учредительном договоре;
- коллективном договоре;
- правилах внутреннего трудового распорядка;
- должностных обязанностях сотрудников;
- специальных нормативных документах по информационной безопасности

(приказах, положениях, инструкциях);

- договорах со сторонними организациями;
- трудовых договорах с сотрудниками;
- иных индивидуальных актах.

При организации ИБ организации руководствуются стандартами, в частности используется ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (Дата актуализации: 21.05.2015) ГОСТ Р ИСО/МЭК 27005-2010.

Стандарт представляет руководство по менеджменту риска информационной безопасности. Стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска. Знание концепций, моделей, процессов и терминологии, изложенных в ИСО/МЭК 27001 и ИСО/МЭК 27002, важно для полного понимания стандарта. Стандарт применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации.

Задания

Ознакомиться с теоретическим материалом.

Построить алгоритм анализа информации, циркулирующей в корпоративной информационной системе.

Проанализировать информацию, циркулирующей в корпоративной информационной системе предприятия.

Построить полную диаграмму информационных потоков предприятия.

Список индивидуальных тем - Банк, Больница, Юридическая фирма, Фирма, занимающаяся маркетинговыми исследованиями, Психологическая клиника, ЗАГС, УФМС, Казначейство, Налоговая инспекция, ВУЗ, Страховая компания, Магазин бытовой техники, Аэропорт, Аптека, Управление дорожного хозяйства.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 5

Сущность учета затрат и калькулирования

Теоретическая часть

Инструменты и механизмы информационной безопасности включают в себя процессы и процедуры ограничения и разграничения доступа, информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); использование методов надежного хранения, преобразования и передачи информации; нормативно-административное побуждение и принуждение.

На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и др.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией др.)., но одних технических средств недостаточно: необходима организационно-управленческая деятельность - организационное обеспечение информационной безопасности, которое

представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации.

Политика безопасности определяется как совокупность документированных управленческих решении, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности;
- адекватность (разумная достаточность);
- системность;
- прозрачность для легальных пользователей;
- равностойкость звеньев.

Главными этапами построения политики безопасности являются следующие:

- обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;

- подготовка персонала работе со средствами защиты;

- организация обслуживания по вопросам информационной безопасности;

- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается Концепция информационной безопасности ИС, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят

отражение следующие основные моменты:

- организация сети организации;

- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;

- организация хранения информации в ИС;

- организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);

- регламентация допуска персонала к той или иной информации;

- ответственность персонала за обеспечение безопасности.

Под обеспечением безопасности информационных систем понимают меры, предохраняющие информационную систему от случайного или преднамеренного вмешательства в режимы ее функционирования.

Существует два принципиальных подхода к обеспечению компьютерной безопасности.

- Фрагментарный. Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.).

Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком - локальность действия, т.е. фрагментарные меры защиты обеспечивают

эффективную защиту конкретных объектов от конкретной угрозы. Но не более того.

- Комплексный. Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам и традиционно рассматривается в виде трех дополняющих друг друга направлений. Организация защищенной среды обработки информации позволяет в рамках существующей политики безопасности обеспечить соответствующий уровень безопасности АИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Задания

Составить перечень мероприятий необходимых для построения комплексной системы защиты конфиденциальной информации (далее по тексту КСЗИ) с учётом нормативно-методических актов.

Написать политику безопасности для выбранного предприятия.

Вопросы к практическому занятию:

1. Назовите закон о защите персональных данных.
2. Каким документом определяются требования к защите персональных данных?
3. Назовите перечень документов используемых для защиты персональных данных.
4. Назовите документ, регламентирующий использование криптографических средств защиты в информационных системах
5. Назовите основные принципы политики безопасности.
6. Что означает принцип эшелонированности обороны?
7. Какие вопросы отражаются в Концепции информационной безопасности?
8. Что включает политика безопасности верхнего уровня?
9. Как организован удаленный доступ к сервису?

10. Что включает политика управления паролями?

11. Как оценить риски реализации угроз информации?

12. Какие этапы выделяются в жизненном цикле информационного сервиса?

13. На каких принципах базируется системный подход к защите информации?

14. Как обеспечивается управление доступом?

15. Какие программные средства используются для ИБ?

16. В чем отличия метода принуждения от метода побуждения?

17. Чем занимается криптография?

18. Что такое электронная подпись и для чего она используется?

19. Политика безопасности и ее принципы.

20. Методы и средства обеспечения информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 6

Организация системы защиты информации

Теоретическая часть

Выделяют 4 основные задачи организационно-управленческой деятельности в сфере информационной безопасности: обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности; обеспечение непрерывности и целостности процессов информационной безопасности; решение методических задач, лежащих в основе эффективного управления информационной безопасностью (вопросов управления рисками, экономического моделирования и т.п..).; управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности. При этом данные задачи должны решаться в комплексе и непрерывно [36].

Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя комплекс задач,

охватывающий все основные аспекты деятельности людей: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п. Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп таких субъектов (партнеров по бизнесу, организаций, которые совместно решают определенные задачи, требующие защиты информации).

Организационное обеспечение - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

Организационное обеспечение компьютерной безопасности включает в себя ряд мероприятий:

- организационно-административные;
- организационно-технические;
- организационно-экономические.

Подключение корпоративных, локальных сетей или отдельных персональных компьютеров к сети Интернет таит в себе определенные угрозы информационной безопасности.

1. Угроза внешних кибератак и, прежде всего, угроза удаленного администрирования.

2. Угроза активного содержимого.

3. Угроза перехвата или подмены данных при их пересылке по открытым каналам связи.

4. Угроза мониторинга и сбора частной информации в интересах третьих лиц.

5. Угроза поставки неприемлемого содержимого.

6. Угроза Интернет-мошенничества.

7. Угроза потери ценной компьютерной информации по различным причинам.

Каждую систему защиты следует разрабатывать индивидуально, учитывая следующие особенности:

- организационную структуру организации;
- объем и характер информационных потоков (внутри объекта в целом, внутри отделов, между отделами, внешних);
- количество и характер выполняемых операций: аналитических и повседневных;
- количество и функциональные обязанности персонала;
- количество и характер клиентов;
- график суточной нагрузки.

Защита должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:

- анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;
- реализация системы защиты на основе результатов анализа риска;
- постоянный контроль за работой системы защиты и АИС в целом (программный, системный и административный).

Задания

Построить модель угроз информационной системы персональных данных (далее по тексту) ИСПДн Вашего предприятия (задание к практическому занятию 4). Для построения модели угроз необходимо проработать теоретический материал и заполнить таблицы 1 и 2.

Таблица 1 - Характеристики для определения исходного уровня защищённости ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий

По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
локальная ИСПДн, развернутая в пределах одного здания			
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;			
ИСПДн, физически отделенная от сети общего пользования			
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск;			
запись, удаление, сортировка;			
модификация, передача			
По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн			
По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн			
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			

ИСПДн, предоставляющая всю базу данных с ПДн			
ИСПДн, предоставляющая часть ПДн			
ИСПДн, не предоставляющая никакой информации			
Количество баллов по уровням			
Процент характеристик ИСПДн по уровням			
Уровень исходной защищённости ИСПДн			
Коэффициент защищённости ИСПДн (Y1}			

Таблица 2 - Модель угроз ИСПДн «предприятия»

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации					
Использование направленных(ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала					
использование "контактных микрофонов" для съема виброакустических сигналов					
использование "лазерных микрофонов" для съема виброакустических сигналов					
использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет "микрофонного эффекта" в ТС обработки ПДн и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений)					
применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки ПДн и ВТСС ВЧ-сигналом					
применение акустооптических модуляторов на базе ВОЛ, находящихся в поле акустического сигнала ("оптических микрофонов")					
Угрозы утечки видовой информации					
визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
использование специальных электронных устройств съема видовой информации (видеозакладки)					
Угрозы утечки информации по каналам ПЭМИН					
применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы					

спектра, селективные микровольтметры)					
применение токосъемников для регистрации наводок информативного сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений					
применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИСПДн или при наличии паразитной генерации в узлах ТС					
применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИСПДн в которых проводится обработка информативных сигналов -параметрических каналов утечки					
Угрозы НСД в ИСПДн					
Угрозы использования уязвимостей ИСПДн					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке СПО и ТС, недекларированные возможности СПО					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке НПО, недекларированные возможности ППО					
неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное)					
сбои в работе ТС и ПО (сбои в электропитании, выход из строя аппаратных элементов, внешние воздействия электромагнитных полей)					
Угрозы непосредственного доступа в операционную среду ИСПДн					
доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя на АРМ					
доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ					
доступ в среду функционирования прикладных программ (локальная СУБД, например)					
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности					
Угрозы программно-математических воздействий:					
внедрение программных закладок					

внедрение вредоносных программ (случайное или преднамеренное, по каналам связи)					
внедрение вредоносных программ (случайное или преднамеренное, непосредственное)					
Угрозы несанкционированного физического доступа к съемным носителям информации					
повреждение носителя информации					
утрата носителя информации					
хищение носителя информации					
Угрозы доступа к ТС и системам обеспечения					
нарушение функционирования кабельных линий связи, оборудования					
нарушение функционирования ТС обработки информации, НЖМД					
доступ к системам обеспечения, их повреждение					
доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)					
Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации					
Несанкционированное изменение информации					
Несанкционированное копирование информации					
Угрозы разглашения информации					
разглашение информации лицам, не имеющим права доступа к ней					
передача защищаемой информации по открытым каналам связи					
копирование информации на незарегистрированный носитель информации, в том числе печать					
передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации					

Вопросы к практическому занятию:

1. Какие организационно-административные меры Вы знаете?
2. Назовите составляющие организационного обеспечения компьютерной безопасности.
3. Что входит в состав организационно-технических мер?
4. Перечислите организационно-экономические меры защиты информации.
5. Какие качества проверяются у лиц при приеме на работу?
6. Что включает конфиденциальное делопроизводство?
7. Для чего применяют межсетевые экраны?
8. Как классифицируются технические средства противодействия?
9. Какие подразделения в службе безопасности?
10. Каковы масштабы применения Интернета в мире?
11. Какие информационные угрозы являются платой за использования Интернета?
12. Назовите меры по защите информации в интернете.
13. Для чего используются межсетевые экраны-брандмауэры?
14. Что используется для защиты электронной почты?
15. Что можно использовать для защиты от вирусов?
16. Какие Вы знаете антивирусные программы?
17. Назовите основные источники проникновения вирусов.
18. Как пакостит «больной» телефон?
19. В чем разница симметричного и ассиметричного шифрования?
20. Какие особенности компании необходимо учитывать при разработке системы защиты?
21. Что необходимо защищать в корпоративной сети?
22. Назовите основные этапы построения системы защиты.
23. Как классифицируют меры обеспечения безопасности по способам осуществления?
24. В чем отличия «встроенной» защиты от «добавленной»?

25. Что делается на этапе сопровождения системы?

26. Назовите критерии оптимального соотношения в анализе различных вариантов построения системы защиты.

27. Что включает план защиты?

28. Дайте характеристику плана обеспечения непрерывной работы и восстановления (ОНРВ).

29. Как оценить эффективность инвестиций в информационную безопасность?

30. Дайте определение политики информационно безопасности.

31. Из каких основных документов состоит политика информационной безопасности?

32. Назовите общее содержание политики разрешения доступа к технологическим ресурсам.

33. Что включает в себя политика пользования электронной почтой?

34. Назовите общее содержание антивирусная политика.

35. Назовите общее содержание политика подготовки, обмена и хранения документов.

36. Что включает в себя политика информационно-технической поддержки?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 7

Управление информационной безопасностью государственных структур. Менеджмент и аудит информационной безопасности на уровне предприятия.

Теоретическая часть

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность

(военных сведений, информации о космических и ядерных технологиях и т.п.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике деятельность органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная стабильность и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают затраты и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и т.п.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- сохранение суверенитета государства;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- укрепление законности и правопорядка;
- обеспечение социально-экономического развития страны и

устойчивости финансовой системы;

участие в жизни международного сообщества.

Обеспечение собственной информационной безопасности на предприятиях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению информационной безопасности становится тем более высокой, чем выше степень автоматизации бизнес-процессов предприятия и чем больше "интеллектуальная составляющая" в его конечном продукте, т.е. чем в большей степени успешность деятельности зависит от наличия и сохранения определенной информации, обеспечения ее конфиденциальности и доступности для владельцев и пользователей.

Так же, как и на государственном уровне, управление информационной безопасностью на уровне предприятий направлено на нейтрализацию различных видов угроз:

- внешних, таких как неправомерные действия государственных органов, противоправная деятельность преступников и преступных группировок, незаконные действия компаний- конкурентов и других хозяйствующих субъектов, недобросовестные действия компаний-партнеров, несоответствие действующей нормативно-правовой базы фактическому развитию технологий и общественных отношений, сбои и нарушения в работе глобальных информационных и телекоммуникационных систем и информационных систем компаний-партнеров и др.;
- внутренних, таких как ошибки и халатность персонала предприятия, а также намеренно допускаемые нарушения, сбои и нарушения в работе собственных информационных систем и др.

Таким образом, управление информационной безопасностью на каждом отдельном предприятии должно осуществляться в контексте его общей хозяйственной деятельности: с учетом характера деятельности компании, а также фактически складывающейся ситуации в рыночной

конкурентной борьбе, государственной политике, развития правовой и правоохранительной системы, уровня развития отдельных используемых информационных и телекоммуникационных технологий и других факторов, формирующих общие условия текущей деятельности.

Задания

Составить перечень внутренних нормативных документов предприятия регламентирующих защиту информацию.

Составить план мероприятий по улучшению информационной безопасности предприятия выбранного в практическом занятии 1.

Вопросы к практическому занятию:

1. Назовите структуру нормативных документов предприятия.
2. Какой документ по защите информации является первичным нормативным актом на предприятии?
3. Перечислите законы, регулирующие порядок работы с конфиденциальной информацией.
4. Что регулирует закон об архивном деле?
5. Что регулирует Федеральный закон "О защите персональных данных"?
6. Что регулирует Федеральный закон "О коммерческой тайне"?
7. Что регулирует Федеральный закон "О связи"?
8. Перечислите общий список внутренних нормативных документов, которые должны быть на любом объекте информатизации?
9. Дайте определение политики информационно безопасности.
10. Из каких основных документов состоит политика информационной безопасности?
11. Назовите общее содержание политики разрешения доступа к технологическим ресурсам.
12. Что включает в себя политика пользования электронной почтой?
13. Назовите общее содержание антивирусная политика.
14. Назовите общее содержание политика подготовки, обмена и

хранения документов.

15. Что включает в себя политика информационно -технической поддержки?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 8

Аудит и менеджмент информационной безопасности электронной коммерции

Теоретическая часть

Количество пользователей Интернета достигло несколько сот миллионов и появилось новое качество в виде «виртуальной экономики». В ней покупки совершаются через торговые сайты, с использованием новых моделей ведения бизнеса, своей стратегией маркетинга и пр.

Электронная коммерция (ЭК) - это предпринимательская деятельность по продаже товаров через Интернет. Как правило выделяются две формы ЭК:

торговля между предприятиями (businesstobusiness, B2B);

торговля между предприятиями и физическими лицами, т.е. потребителями (businesstoconsumer, B2C).

ЭК породила такие новые понятия как:

Электронный магазин - витрина и торговые системы, которые используются производителями или дилерами при наличии спроса на товары.

Электронный каталог - с большим ассортиментом товаров от различных производителей.

Электронный аукцион - аналог классического аукциона с использованием Интернет- технологий, с характерной привязкой к мультимедийному интерфейсу, каналу доступа в Интернет и показом особенностей товара.

Электронный универмаг - аналог обычного универмага, где обычные фирмы выставляют свой товар, с эффективным товарным брендом (Гостиный двор, ГУМ и т.д.).

Виртуальные комъюнити (сообщества), в которых покупатели

организуются по группам интересов (клубы болельщиков, ассоциации и т.д.).

Существует несколько видов угроз электронной коммерции:

- Проникновение в систему извне.

- Несанкционированный доступ внутри компании.

- Преднамеренный перехват и чтение информации.

- Преднамеренное нарушение данных или сетей.

- Неправильная (с мошенническими целями) идентификация пользователя.

- Взлом программно-аппаратной защиты.

- Несанкционированный доступ пользователя из одной сети в другую.

- Вирусные атаки.

- Отказ в обслуживании.

- Финансовое мошенничество.

Для противодействия этим угрозам используется целый ряд методов, основанных на различных технологиях, а именно: шифрование - кодирование данных, препятствующее их прочтению или искажению; цифровые подписи, проверяющие подлинность личности отправителя и получателя; stealth-технологии с использованием электронных ключей; брандмауэры; виртуальные и частные сети.

Вопросы к практическому занятию:

1. Для чего используется электронная цифровая подпись в системе электронных платежей?
2. Назовите особенности электронной коммерции.
3. В чем отличия электронного магазина от электронного каталога?
4. Какие выгоды приносит Интернет в сфере электронной коммерции?
5. Какие способы доставки и оплаты товара в ЭК?
6. В чем состоит проблема информационной безопасности ЭК?
7. Назовите основные угрозы ЭК.
8. Что включает комплексная система ИБ ЭК?

Список рекомендуемой литературы

Основная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html

3. Садыков, А. М. Введение в информационную безопасность: основы, методы, задачи : практикум / А. М. Садыков, А. Р. Касимова, А. А. Алексеева. — Казань : Казанский национальный исследовательский технологический университет, 2024. — 92 c. — ISBN 978-5-7882-3573-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/158934.html

Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации Электронный ресурс : Учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Информационная безопасность и защита информации,2019-02-17. - Москва : Евразийский открытый институт, 2012. - 311 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-374-00301-7, экземпляров неограничено

2. Полетайкин, А.Н. Социальные и экономические информационные системы. Законы функционирования и принципы построения Электронный ресурс : учебное пособие / А.Н. Полетайкин. - Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2016. - 241

с. - Книга находится в базовой версии ЭБС IPRbooks.

3. Гринберг, А. С. Информационный менеджмент / А.С. Гринберг ; И.А. Король. - Москва : Юнити-Дана, 2015. - 415 с. - (Профессиональный учебник: Информатика). - ISBN 5-238-00614-4

4. Алексеев, А.П. Многоуровневая защита информации Электронный ресурс : монография / А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. - 128 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-904029-72-2, экземпляров неограничено

5. Международная информационная безопасность : новая геополитическая реальность : монография / Московский государственный институт международных отношений (Университет) МИД России, Центр международной информационной безопасности и научно-технологической политики ; под редакцией Е. С. Зиновьевой, М. Б. Алборовой. - Москва : Аспект Пресс, 2021. - 112 с. : табл. - РФФИ. - Библиогр. в конце гл. - ISBN 978-5-7567-1129-5

Интернет-ресурсы:

1. http:// finansy.ru/ - Экономика и финансы-публикации, статьи, обзоры, аналитика, прогнозы

2. http://analytics.interfax.ru - Интернет сайт Бюро экономического анализа ИА «Интерфакс»

3. http://investaki.ru/ - Ваш финансовый консультант;

4. http://rusg2b.ru/library/useful/ , http://library.infosoc.ru - публикации электронной библиотеки «Технологии информационного общества в России»;

5. Информационная справочная система ГАРАНТ.РУ // Режим доступа: http://www.garant.ru/

6. Информационная справочная система КонсультантПлюс. // Режим доступа:http://www.consultant.ru

7. Профессиональная база данных «Всероссийская система данных о

компаниях и бизнесе «За честный бизнес» // Режим доступа: https://zachestnyibiznes.ru.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Информационная безопасность организаций»
для студентов направления подготовки 38.04.01 Экономика
направленность (профиль) «Экономическая безопасность и управление рисками»

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы
по дисциплине «Информационная безопасность организаций»
для студентов направления подготовки 38.04.01 Экономика
направленность (профиль) «Экономическая безопасность и управление рисками»

2026

Данные методические указания предназначены для оказания помощи студентам при изучении дисциплины. Работа содержит требования к выполнению индивидуального творческого проекта, порядок выполнения и защиты, рекомендации по оформлению.

Методические указания предназначены для студентов направления подготовки 38.04.01 Экономика направленность (профиль) «Экономическая безопасность и управление рисками».

Индивидуальный творческий проект (ИТП) - самостоятельная работа студента, основной целью и содержанием которой является развитие навыков теоретических исследований, обобщений, оценка результатов исследований.

Индивидуальный творческий проект должен отразить умение студента с помощью системного анализа и осмысления фактического материала исследовать избранную тему и грамотно изложить результаты исследования.

Целью подготовки ИТП по дисциплине является глубокое изучение и усвоение предмета по одной из тем.

ИТП должен представлять собой самостоятельное изложение существа (содержания) основных вопросов избранной темы. Выполнение ИТП должно помочь студенту:

- научиться подбирать литературу по определенной теме;
- содействовать развитию и закреплению навыков теоретического и практического использования различных источников: учебной литературы, научных работ, нормативно-законодательных актов, статистических материалов;
- на основе полученных знаний выполнять теоретическую разработку избранной темы;
- выработать умение самостоятельно формулировать свои мысли и выводы, логично и последовательно доказывать их, уметь анализировать;
- научиться: правильно оформлять научно-справочный материал;
- выработать умение публичной защиты подготовленной работы (сделать доклад, дать ответы на вопросы, отстаивать свое мнение и т. д.).

1 ФОРМУЛИРОВКА ЗАДАНИЯ И ЕГО ОБЪЕМ

Наиболее важным и ответственным моментом, предопределяющим успех в подготовке ИТП, является выбор темы.

Темы ИТП охватывают наиболее актуальные проблемы в области изучения дисциплины. Тематика ИТП составлена в соответствии с программой по дисциплине и выдается студентам, в начале семестра. Тема ИТП выбирается студентами самостоятельно, по желанию, или выдается преподавателем. Прежде чем приступить к написанию ИТП, необходимо ознакомиться с заданием и подобрать необходимую литературу. После выбора темы составляется список литературы, опубликованных статей, необходимых справочных источников. Подобранную литературу следует зафиксировать согласно ГОСТ по библиографическому описанию произведений печати. Подобранная литература изучается в следующем порядке:

- знакомство с литературой, просмотр ее и выборочное чтение с целью общего представления проблемы и структуры будущей научной работы;

- исследование необходимых источников, сплошное чтение отдельных работ, их изучение, конспектирование необходимого материала;

- обращение к литературе для дополнений и уточнений на этапе написания ИТП.

Для разработки ИТП достаточно изучение 4 - 5 важнейших источников по избранной проблеме. При изучении литературы необходимо выбирать материал, не только подтверждающий позицию автора ИТП, но и материал для полемики.

Тематика ИТП разрабатывается, утверждается кафедрой и предоставляется студентам для ознакомления.

Объем ИТП ориентировочно доставляет 20 - 25 страниц рукописного или 15-20 страниц напечатанного текста (межстрочное расстояние - полуторное; размер шрифта. - 14 пунктов).

2 ОБЩИЕ ТРЕБОВАНИЯ К НАПИСАНИЮ ИТП

ИТП должен отвечать следующим требованиям. По содержанию:

1) в ИТП должны присутствовать характерные поисковые признаки:

- раскрытие содержания основных концепций;
- цитирование мнений некоторых специалистов поданной проблеме;
- материал следует излагать кратко, не допуская дословного переписывания текста из литературных источников;

2) при обработке полученного материала автор должен:

- систематизировать его по разделам;
- выдвинуть и обосновать свои гипотезы;
- определить свою позицию, точку зрения по рассматриваемой проблеме;
- уточнить объем и содержание понятий, которыми приходится оперировать при разработке темы;
- сформулировать определения и основные выводы, характеризующие результаты исследования;
- окончательно уточнить структуру ИТП.

3) при использовании цитат, статистических и исторических данных и т. п. необходимо делать сноски с указанием источника: автор, название книги, место издания, год издания, страница цитируемого материала;

4) ИТП должен включать в себя:

- титульный лист;
- содержание, которое должно иметь внутреннее единство, строгую логику изложения, смысловую завершенность раскрываемой темы;
- введение, где обосновывается актуальность проблемы, сопоставляются основные точки зрения, ставятся цель и задачи исследования;
- основную часть, в которой раскрывается содержание проблемы. В

основной части формулируются ключевые понятия и положения, вытекающие из анализа теоретических источников (теоретических точек зрения, моделей, концепций), документальных источников *к* материалов практики, экспертных сделок по вопросам исследуемой проблемы, а также результатов эмпирических исследований. ИТП носит исследовательский характер, содержит результат творческого поиска автора;

- заключение, в котором формулируются главные итоги авторского исследования в соответствии с выдвинутой целью и задачами ИТП, излагаются обобщенные выводы или практические рекомендации по разрешению исследуемой проблемы в рамках государства, регионального уровня или уровня конкретной организации;
- список использованных источников;
- приложения - при необходимости.

ИТП относится к текстовым документам и должен соответствовать требованиям ГОСТ 2.105-95. ЕСКД. Общие требования к текстовым документам и ГОСТ 2.106-96. ЕСКД. Текстовые документы. Текст ИТП может быть выполнен как в рукописном виде, так и с применением средств оргтехники.

При выполнении работы в рукописном виде почерк должен быть легко читаем, не содержать не установленных сокращений и не создавать затруднений при проверке. При изложении материала необходимо придерживаться принятого плана.

Работа выполняется на листах формата А 4 (210 х 297 мм) с указанием нумерации листов (сверху, по центру); шрифт Times New Roman, размер -14; междустрочный интервал - полуторный; с соблюдением трафаретов (полей): слева - 30 мм; справа - 1 5 мм; сверху - 20 мм; снизу - 20 мм.

Содержание оформляется в виде перечня разделов и подразделов ИТП с указанием номера страницы, с которой они начинаются.

Разделы ИТП нумеруются арабскими цифрами, подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из

номера раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится (например, 1.1; Г. 1.1). Разделы и подразделы должны иметь названия. Подчеркивание, раскрашивание и перенос слов в заголовках не допускается. Каждый раздел следует начинать с новой страницы. Нумерация страниц должна быть сплошной: первой страницей является титульный лист, второй - содержание ИТП и т. д. Цифровой материал оформляется, как правило, в виде таблиц. Номер таблицы и; ее название помещается над таблицей с абзацного отступа. Внизу под таблицей (а не снизу страницы) необходимо указать источники данных. Иллюстрации обозначаются словом «Рисунок» и нумеруются последовательно арабскими цифрами сквозной нумерацией. Приложения следует помещать после текстового материала и обозначать заглавными буквами русского алфавита, начиная с А.

3 РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ РАБОТ НАД ЗАДАНИЕМ, ПРИМЕРНЫЙ КАЛЕНДАРНЫЙ ПЛАН ЕГО ВЫПОЛНЕНИЯ

Прежде чем приступить к написанию ИТП, студенту необходимо по выбранной теме задания изучить рекомендуемую как основную, так и дополнительную литературу, а также периодическую печать. Затем приступать к написанию работы.

Подготовка ИТП - это особый вид работы с литературой, прежде всего научной. Изучение литературы по теме следует начинать с учебников и учебных пособий, которые более доступны и позволяют определить круг рассматриваемых вопросов избранной темы. Однако эти источники не могут быть использованы в качестве теоретической основы ИТП. Являясь самостоятельным исследованием, он должен опираться на научную, монографическую литературу, а также журнальные статьи. Работа с монографиями включает ознакомление с заглавиями, аннотациями, предисловиями, в которых содержатся данные о структуре издания, его

актуальности и отличие от других работ.

Подобный подход позволяет за максимально короткий срок определить ценность библиографических источников и составить их список.

Предварительное общее знакомство с литературой чрезвычайно полезно. Проведя систематизацию изученных работ, студент одновременно определяет способы будущей обработки того или иного материала. Изучение вопросов темы лучше начинать с основных обобщающих работ, постепенно переходя к специальным исследованиям. При изучении научной литературы надо обязательно обращать внимание на научно-справочный аппарат: примечания, подстрочные ссылки, библиографию, приложение и т. д.

Изучение специальной литературы может производиться двумя способами. В каждой научной работе материал, относящийся к теме, прочитывается и осмысливается сразу по всем вопросам. В этом случае после изучения каждого такого источника у студента складывается более или менее цельное представление о содержании ИТП. Но при таком способе труднее акцентировать внимание на каждом его вопросе в отдельности. Поэтому применяем и другой способ - изучение литературы по каждому отдельному вопросу.

При изучении литературы нужно записывать все встречающиеся спорные вопросы, выявлять точки зрения различных авторов, с тем чтобы, сопоставив их, получить правильное представление.

Изучив необходимую по данной проблеме литературу, автор должен разобраться в имеющихся точках зрения, показать умение обобщать, систематизировать, сопоставлять, кратко и концептуально излагать и оценивать идеи различных авторов и на этой основе формулировать собственную точку зрения или присоединяться к одной из изложенных в научных работах.

После ознакомления с литературой студент составляет план ИТП. План работы есть отображение ее структуры, под которой понимается порядок построения и взаимосвязь ее частей. Следует отметить, что часто встречается

такой недостаток, как несоразмерность глав, разделов темы, что объясняется увлечением какой-то одной проблемой в ущерб другим.

ИТП рекомендуется выполнять в соответствии с графиком выполнения, предложенным преподавателем. На основе графика студент сам должен планировать ход своего исследования, которое включает индивидуальное составление календарного плана научного исследования и плана предполагаемого ИТПе..

Календарный план исследования включает следующие элементы:

- выбор и формулирование проблемы, разработка плана исследования и предварительного плана ИТП;
- сбор и изучение неходкого материала, подбор литературы;
- анализ собранного материала, теоретическая разработка проблемы;
- сообщение о предварительных результатах исследования;
- литературное оформление исследовательской проблемы;
- обсуждение работы (на практических занятиях, в студенческом Научном обществе, на конференции и т. п.).

4 ПОРЯДОК ЗАЩИТЫ И ОТВЕТСТВЕННОСТЬ СТУДЕНТА ЗА ВЫПОЛНЕНИЕ ЗАДАНИЯ

ИТП должен быть представлен к защите согласно графику выполнения работы. Работа должна быть выполнена по выбранной теме, в противном случае она возвращается без проверки. Студент может получить консультацию на кафедре от преподавателя, который проверяет ИТП.

Защита ИТП проводится в устной форме и предполагает проверку знаний студента относительно теоретической части задания, кроме того, по теме ИТП преподавателем и студентами группы задаются дополнительные вопросы. Перед защитой студент готовится как по работе в целом, так и по замечаниям преподавателя. На защите студент должен хорошо ориентироваться в вопросах темы, уметь объяснить основные положения как теоретического, так и практического характера, относящиеся к теме работы.

Содержание ИТП может быть изложено студентом на одном из практических занятий и обсуждено в группе. В конце своего сообщения студент отвечает на замечания преподавателя, сделанные им при проверке ИТП, и вопросы сокурсников. При оценке учитывается качество написанной работы и результаты ее защиты. В случае, когда студент не выполняет задание по написанию ИТП, то он не допускается к сдаче экзамена (зачета).

Студенты, подготовившие наиболее удачные ИТП, могут быть рекомендованы к участию в студенческих научных конференциях.

Оценка ИТП определяется по четырехбалльной системе: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно» и зависит от знания студентом сути проблемы и умения грамотно отвечать на вопросы и критические замечания.

5 ОФОРМЛЕНИЕ СПИСКА ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Список использованной литературы должен содержать перечень источников, использованных при выполнении работы, с указанием авторов, наименования, места издания, издательства, года выпуска и количества страниц.

Схема расположения материала в библиографическом списке (литература):

Официальные материалы:

- конституция;
- кодексы;
- законы;
- указы;
- постановления;
- труды, речи, выступления государственных деятелей;
- источники статистических данных;
- ведомственные положения, инструкции, письма.

Отечественная литература:

В алфавите фамилии авторов или заглавий книг и статей.

Иностранная литература:

В латинском алфавите.

Допускается также использование источника информации из глобальной сети Интернет с указанием адреса.

6 ТЕМАТИКА ИНДИВИДУАЛЬНЫХ ТВОРЧЕСКИХ ПРОЕКТОВ

ИТП (сроки выполнения 1-16 недели, выдача задания – 1 неделя) выполняется по следующей тематике:

Базовый уровень

1. Информационное право и информационная безопасность.

2. Концепция информационной безопасности.

3. Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

5. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

6. Информационная безопасность (по материалам зарубежных источников и литературы).

7. Правовые основы защиты конфиденциальной информации.

8. Экономические основы защиты конфиденциальной информации.

9. Организационные основы защиты конфиденциальной информации.

10. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

11. Составление инструкции по обработке и хранению конфиденциальных документов.

12. Направления и методы защиты документов на бумажных

носителях.

13. Направления и методы защиты машиночитаемых документов.

14. Архивное хранение конфиденциальных документов.

15. Направления и методы защиты аудио- и визуальных документов.

16. Порядок подбора персонала для работы с конфиденциальной информацией.

17. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

18. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

19. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

Повышенный уровень

1. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

2. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

3. Порядок защиты информации в рекламной и выставочной деятельности.

4. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

5. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

6. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

7. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

8. Назначение, виды, структура и технология функционирования

системы защиты информации.

9. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

10. Аналитическая работа по выявлению каналов утечки информации фирмы.

11. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

12. Направления и методы защиты профессиональной тайны.

13. Направления и методы защиты служебной тайны.

14. Направления и методы защиты персональных данных о гражданах.

15. Методы защиты личной и семейной тайны.

16. Построение и функционирование защищенного документооборота.

17. Защита секретов в дореволюционной России.

18. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Задания для самоконтроля

Номер задания	**Содержание оценочного средства**	**Компетенция**
	Тестовые задания	
1.	Информационная безопасность - это... a) невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз); b) предотвращение зла наносимого государственным структурам; c) проведение природоохранных мероприятий.	ПК-5
2.	К объектам информационной безопасности на предприятии НЕ относятся:	ПК-5

	a) информационные ресурсы; b) средства вычислительной и организационной техники; c) Конституция России.	
3.	К основным угрозам информационной безопасности НЕ относятся: a) раскрытие конфиденциальной информации; b) нарушение принципов экономической безопасности; c) отказ от обслуживания.	ПК-5
4.	Конфиденциальность – это.. a) защита от несанкционированного доступа к информации b) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов c) описание процедур	ПК-5
5.	В организационную основу системы обеспечения информационной безопасности РФ входит: a) Совет безопасности РФ; b) Министерство науки и высшего образования РФ; c) ЦРУ США.	ПК-5
6.	Правовое обеспечение безопасности информации делится: a) международно-правовые нормы; b) национально-правовые нормы; c) все ответы правильные.	ПК-5
7.	Что относится к государственной тайне? a) сведения, защищаемые государством в области военной, экономической … деятельности b) документированная информация c) нет правильного ответа	ПК-5
8.	Угрозы можно классифицировать по нескольким критериям: a) по спектру информационной безопасности b) по способу осуществления c) по компонентам информационной системы d) все варианты верны	ПК-5
9.	Основными источниками внутренних отказов являются: a) отступление от установленных правил эксплуатации b) разрушение данных c) ошибки при конфигурировании системы	ПК-5

	d) отказы программного или аппаратного обеспечения e) выход системы из штатного режима эксплуатации f) все ответы правильные	
10.	По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы: a) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности b) обрабатывать большой объем программной информации c) нет правильного ответа	ПК-5
11.	Политика безопасности разрабатывается применительно к a) Одному верхнему уровню управления; b) Трем уровням управления (верхнему, среднему и нижнему); c) Решению акционеров компании.	ПК-5
12.	Какие угрозы безопасности информации являются преднамеренными: a) ошибки персонала b) открытие электронного письма, содержащего вирус c) не авторизованный доступ	ПК-5
13.	Минимизация утечки информации через персонал это a) организационно-технические средства защиты информации; b) организационно-экономические меры; c) организационно-административные меры.	ПК-5
14.	К организации конфиденциального делопроизводства относится: a) организация документооборота; b) использование сертифицированных технических и программных средств; c) проверка надежности сотрудников.	ПК-5
15.	Не являются коммерческой тайной: a) сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью; b) сведения о научных разработках; c) сведения о персонале предприятия.	ПК-5
	Вопросы к экзамену	
16.	Экономическая информация как товар и объект безопасности.	ПК-5
17.	Информационные угрозы, их виды и причины возникновения.	ПК-5

18.	Информационные угрозы для государства.	ПК-5
19.	Внешние и внутренние субъекты информационных угроз.	ПК-5
20.	Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.	ПК-5
21.	Информационные угрозы для государства.	ПК-5
22.	Информационные угрозы для компании.	ПК-5
23.	Организационное обеспечение информационной безопасности.	ПК-5
24.	Организация системы защиты информации экономических объектов.	ПК-5
25.	Управление информационной безопасности на государственном уровне.	ПК-5
26.	Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.	ПК-5
27.	Способы воздействия информационных угроз на объекты.	ПК-5
28.	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.	ПК-5
29.	Государственное регулирование информационной безопасности.	ПК-5
30.	Федеральные законы по информационной безопасности в РФ.	ПК-5
31.	Организационно-правовой статус службы безопасности.	ПК-5

7. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html

3. Садыков, А. М. Введение в информационную безопасность: основы, методы, задачи : практикум / А. М. Садыков, А. Р. Касимова, А. А.

Алексеева. — Казань : Казанский национальный исследовательский технологический университет, 2024. — 92 c. — ISBN 978-5-7882-3573-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/158934.html

Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации Электронный ресурс : Учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Информационная безопасность и защита информации,2019-02-17. - Москва : Евразийский открытый институт, 2012. - 311 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-374-00301-7, экземпляров неограничено

2. Полетайкин, А.Н. Социальные и экономические информационные системы. Законы функционирования и принципы построения Электронный ресурс : учебное пособие / А.Н. Полетайкин. - Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2016. - 241 c. - Книга находится в базовой версии ЭБС IPRbooks.

3. Гринберг, А. С. Информационный менеджмент / А.С. Гринберг ; И.А. Король. - Москва : Юнити-Дана, 2015. - 415 c. - (Профессиональный учебник: Информатика). - ISBN 5-238-00614-4

4. Алексеев, А.П. Многоуровневая защита информации Электронный ресурс : монография / А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. - 128 c. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-904029-72-2, экземпляров неограничено

5. Международная информационная безопасность : новая геополитическая реальность : монография / Московский государственный институт международных отношений (Университет) МИД России, Центр международной информационной безопасности и научно-технологической политики ; под редакцией Е. С. Зиновьевой, М. Б. Алборовой. - Москва :

Аспект Пресс, 2021. - 112 с. : табл. - РФФИ. - Библиогр. в конце гл. - ISBN 978-5-7567-1129-5

Интернет-ресурсы:

1. http:// finansy.ru/ - Экономика и финансы-публикации, статьи, обзоры, аналитика, прогнозы

2. http://analytics.interfax.ru - Интернет сайт Бюро экономического анализа ИА «Интерфакс»

3. http://investaki.ru/ - Ваш финансовый консультант;

4. http://rusg2b.ru/library/useful/ , http://library.infosoc.ru - публикации электронной библиотеки «Технологии информационного общества в России»;

5. Информационная справочная система ГАРАНТ.РУ // Режим доступа: http://www.garant.ru/

6. Информационная справочная система КонсультантПлюс. // Режим доступа:http://www.consultant.ru

7. Профессиональная база данных «Всероссийская система данных о компаниях и бизнесе «За честный бизнес» // Режим доступа: https://zachestnyibiznes.ru.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы
по дисциплине «Информационная безопасность организаций»
для студентов направления подготовки 38.04.01 Экономика
направленность (профиль) «Экономическая безопасность и управление рисками»